

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-280724

(P2004-280724A)

(43) 公開日 平成16年10月7日(2004.10.7)

(51) Int.Cl.⁷
G06F 13/00
G06F 15/00
H04L 12/22

F 1
G06F 13/00
G06F 15/00
H04L 12/22

テーマコード(参考)

5B085
5B089
5K030

審査請求 未請求 請求項の数 10 O.L. (全 33 頁)

(21) 出願番号 特願2003-74546 (P2003-74546)
(22) 出願日 平成15年3月18日 (2003.3.18)

(出願人による申告) 国等の委託研究の成果に係る特許出願(平成14年度通信・放送機器「サービス不能化(DDoS)攻撃に対する防御技術に関する研究開発」委託研究、産業活力再生特別措置法第30条の適用を受けるもの)

(71) 出願人 000005223
富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番1号

(74) 代理人 100074099
弁理士 大曾 義之

(74) 代理人 100067987
弁理士 久木元 彰

(72) 発明者 田村 直広
神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

(72) 発明者 羽生 卓哉
神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

最終頁に続く

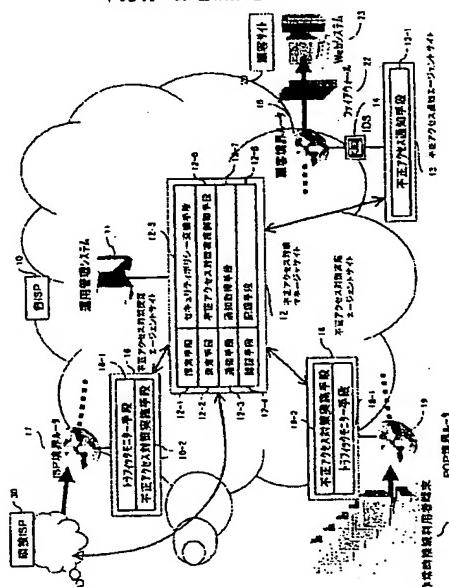
(54) 【発明の名称】不正アクセス対処システム、及び不正アクセス対処処理プログラム

(57) 【要約】

【課題】不正アクセス発信元にできるだけ近い場所で不正アクセス対策を実施することにより、分散型サービス不能化攻撃に効果的に対処する。

【解決手段】自 ISP 10 より公開されている Web システム 21 によるサービスに対する不正なアクセスの流入路の探索を行う探索手段 12-1 と、このサービスをこの不正なアクセスから保護するための対策を実施する場所の決定をこの探索の結果に基づいて行う決定手段 12-2 と、この不正なアクセスを自己の通信ネットワークに流入させている流入元でこの対策を実施するとの決定に応じて該決定を該流入元へ通知する通知手段 12-3 と、を有する。

本発明の原理構成を示す図



【特許請求の範囲】

【請求項1】

自己の通信ネットワークより公開されているサービスに対する不正なアクセスの流入路の探索を行う探索手段と、前記サービスを前記不正なアクセスから保護するための対策を実施する場所の決定を前記探索の結果に基づいて行う決定手段と、前記不正なアクセスを自己の通信ネットワークに流入させている流入元で前記対策を実施するとの前記決定に応じて該決定を該流入元へ通知する通知手段と、を有することを特徴とする不正アクセス対処システム。

【請求項2】

自己の通信ネットワークより公開されているサービスに対する不正なアクセスの流入路の探索を行う探索処理と、前記サービスを前記不正なアクセスから保護するための対策を実施する場所の決定を前記探索の結果に基づいて行う決定処理と、前記不正なアクセスを自己の通信ネットワークに流入させている流入元で前記対策を実施するとの前記決定に応じて該決定を該流入元へ通知する通知処理と、を 컴퓨터に行わせるための不正アクセス対処処理プログラム。

【請求項3】

前記探索処理は、前記自己の通信ネットワークで伝送されているトライフィックの監視情報と前記不正なアクセスの内容を示す不正アクセス情報とに基づいて前記流入路を探索する処理を前記コンピュータに行わせることを特徴とする請求項2に記載の不正アクセス対処処理プログラム。

【請求項4】

前記通知処理は、前記不正なアクセスの流入元との間で各々のネットワーク運用におけるセキュリティポリシーに関する情報を交換した後に前記決定を該流入元へ通知する処理を前記コンピュータに行わせることを特徴とする請求項2に記載の不正アクセス対処処理プログラム。

【請求項5】

前記通知処理は、前記不正なアクセスの流入路とは異なる通信経路を用いて前記決定を該不正なアクセスの流入元へ通知する処理を前記コンピュータに行わせることを特徴とする請求項2に記載の不正アクセス対処処理プログラム。

【請求項6】

前記通知処理は、前記自己の通信ネットワークに前記不正なアクセスを流入させている流入元で前記対策を実施する決定がされたときに、該決定を該流入元へ通知するか否かの判定を前記コンピュータに行わせ、前記通知処理の実行によって前記決定を前記流入元へ通知しないとの判定がされたときに、前記サービスを前記

不正なアクセスから保護するための対策を前記自己の通信ネットワーク内で実施させる不正アクセス対策実施制御処理を前記コンピュータに更に行わせる、ことを特徴とする請求項2に記載の不正アクセス対処処理プログラム。

【請求項7】

前記自己の通信ネットワーク内で前記対策を実施するとの前記決定に応じて、該サービスを該不正なアクセスから保護するための対策を該自己の通信ネットワーク内で実施させる不正アクセス対策実施制御処理を前記コンピュータに更に行わせることを特徴とする請求項2に記載の不正アクセス対処処理プログラム。

【請求項8】

前記不正アクセス対策実施制御処理は、前記不正なアクセスの発信元が接続しているPOP(ポイント・オブ・プレゼンス)境界ルータにおいて前記対策を実施させるための処理を前記コンピュータに行わせることを特徴とする請求項7に記載の不正アクセス対処処理プログラム。

20 【請求項9】

前記不正アクセス対策実施制御処理の実行によって実施させた前記対策は、前記不正アクセスの検知がされなくなったときから予め設定されている時間が経過した後には解除されることを特徴とする請求項7に記載の不正アクセス対処処理プログラム。

【請求項10】

前記自己の通信ネットワークとは異なる他の通信ネットワークより公開されているサービスに対する不正なアクセスを該他の通信ネットワークへ流入させている決定の通知を取得する通知取得処理を前記コンピュータに更に行わせ、

前記探索処理は、前記通知取得処理によって前記通知が取得されたときには、該通知に係る不正なアクセスの自己の通信ネットワークにおける流入路を探索する処理を前記コンピュータに行わせ、

前記決定処理は、前記通知取得処理によって前記通知が取得されたときには、前記他の通信ネットワークより公開されているサービスを該通知に係る不正なアクセスから保護するための対策を実施する場所を前記探索の結果に基づいて決定する処理を前記コンピュータに行わせ、前記通知処理は、前記通知取得処理によって前記通知が取得されたときには、該通知に係る不正なアクセスを前記自己の通信ネットワークに流入させている流入元で前記対策を実施する決定に応じて該決定を該流入元へ通知する処理を前記コンピュータに行わせる、ことを特徴とする請求項2に記載の不正アクセス対処処理プログラム。

【発明の詳細な説明】

【0001】

50 【発明の属する技術分野】

3

本発明は、通信ネットワークにおける不正アクセス対策技術に関し、特に、例えばインターネットサービスプロバイダ（ISP）が顧客に提供する不正アクセス対策サービスの実施技術に関するものであり、とりわけ、分散型サービス不能化攻撃に代表される不正アクセス攻撃に対して効果的な対策実施技術に関するものである。

【0002】

【従来の技術】

サービス不能化攻撃（DoS：Denial of Services）とは、故意にシステムリソース許容限度を越えた処理要求を送出することにより、システムを停止または不能化させる攻撃で、正当な処理要求と不当な処理要求との区別が難しいという特徴がある。その内特に攻撃元がネットワーク上に多数分散している形態の攻撃を分散型サービス不能化攻撃（DDoS：Distributed Denial of Service、以下「DDoS攻撃」と称する）という。このDDoS攻撃については非特許文献1に詳説されている。

【0003】

DDoS攻撃に対する従来の対処技術を分類すると下記の2つの手法に大別することができ、その各々の手法について各対処技術を更に細分化することができる。

【0004】

I. 現状のネットワークで使用されている構成要素を置き換える手法

(1) IPパケットを拡張して行われる対処技術
これは、IPパケットにその往復の経路情報を追加すると共に、ルータ（Router）やファイアウォール（Firewall）を現状のものからこの拡張されたIPパケットを理解できるものに置き換えることにより、攻撃元の探索や要求処理の送信元毎の均等化を可能とする技術である。

【0005】

(2) IPパケットの拡張は行わない対処技術
この技術に含まれるものとして、例えば特許文献1で開示されている技術は、境界ルータ（Edge Router）において増殖させて各ルータへ送付するパケットフィルタリングプログラムを受信したルータでそのプログラムを実行して攻撃元からのトラフィックを遮断するというものであり、現状のネットワークで使用されているものに代えてこのプログラムを受信・実行可能なルータが用いられる。

【0006】

II. 現状のネットワークで用いられている構成要素をそのまま使用する手法

この手法について図15を参照しながら説明する。
図15に示したネットワーク構成例において、顧客サイト1000はWebシステム1001を運用しており、更に、Webシステム1001への不正侵入を防護するためのファイアウォール1002を設置している。

【0007】

Webシステム1001はファイアウォール1002を介して境界ルータ2001に接続されている。境界ルータ2001はインターネットサービスプロバイダであるISP-A2000によって管理されている。

【0008】

また、このWebシステム1001に対してDDoS攻撃を行うことを目論んでいる攻撃者は、ネットワーク上でISP-A2000に隣接しているインターネットサービスプロバイダであるISP-B3000によって管理されているPOP（Point of Presence）境界ルータにアクセスしてWebシステムへの攻撃を行う。

【0009】

一方、このWebシステム1001のサービスを利用する正規の利用者は、ネットワーク上でISP-A2000に隣接しているインターネットサービスプロバイダであるISP-C3000の管理しているPOP境界ルータにアクセスしてWebシステム1001によるサービスの提供を受ける。

【0010】

(1) 攻撃対象顧客サイトによる対処技術
これは、IDS（Intrusion Detection System：侵入検知システム）で利用されている不正アクセス検知技術とファイアウォールやルータで利用されているパケット制御（フィルタリングや流量制御など）技術とを実装した装置をISP-A2000と顧客サイト1000とのネットワーク境界に配置（図15においては境界ルータ2001に配置）し、DDoS不正アクセスを検知すると、ISP-A2000から顧客サイト1000へ流れる特定の不正パケットのみを遮断する技術である。

【0011】

(2) 単独ISPによる対処技術
これは、IDS装置をISP-A2000と顧客サイト1000とのネットワーク境界に配置（図15においては境界ルータ2001に配置）し、且つパケット制御装置をISP-A2000と隣接ISPとのネットワーク境界（図15においては境界ルータ2002、2003に配置）に配置し、IDSが不正アクセスを検知すると、送信元を偽った攻撃パケットの上流を特定するIPトレースバック（Traceback）技術を利用して、そのパケットの流入元を特定し、隣接ISPとの境界（図15においては境界ルータ2002）で不正パケットのみを遮断する技術である。

【0012】

(3) 複数ISP連携による対処技術
これは、前述した単独ISPによる対処技術により不正アクセスパケット流入元の隣接ISPがISP-B3000であることを特定したISP-A2000の管理者

5

が、電話による手作業でISP-B3000の管理者へ対策を依頼することにより実現する。ゆえに、現状未確立の技術である。

【0013】

なお、DDoS攻撃に関する技術情報の所在は非特許文献2が詳しい。

ところで、分散型サービス不能化攻撃に対しては、攻撃発信元から攻撃対象顧客サイトへ至る経路上における攻撃発信元により近い場所で対処した方が、より効果的な対策になるといえる。なぜならば、攻撃対象サイトにより近い場所で対策を実施した場合には、攻撃対象サイトを守ることはできるものの、経路上のネットワークの輻輳やルータ処理遅延による不能化が防げないため、そのサイトのサービスをインターネットから利用している者にとっては結局サービスが無効化されたときと同様の状態になってしまうからである。

【0014】

【特許文献1】

特開2002-164938号公報

【非特許文献1】

ケビン・J・ホール (Kevin J Houle)、ジョージ・M・ウィーバ (George M. Weaver) 共著、「トレンド・イン・デナイアル・オブ・サービス・アタック・テクノロジ (Trends in Denial of Service Attack Technology)」、[online]、2001年10月、サート・コーディネーション・センター (CERT Coordination Center)、[平成15年2月17日検索]、インターネット<URL: http://www.cert.org/archive/pdf/DoS_trends.pdf>

【0015】

【非特許文献2】

デイブ・ディトリッヂ (Dave Dittrich)、「ディストリビューティッド・デナイアル・オブ・サービス (ディーディーオーエス)・アタックスツールズ (Distributed Denial of Service (DDoS) Attacks/tools)」、[online]、[平成15年2月17日検索]、インターネット<URL: http://staff.washington.edu/dittrich/misc/ddos/>

【0016】

【発明が解決しようとする課題】

上述した手法のうち、I. の手法においては、新しいプロトコルを実装したルータを現状のネットワークで使用されているものに代えて設置しなければDDoS攻撃に対処できないため、ルータの置き換えの費用がかかる。

更に、新しいプロトコルとその新プロトコルを扱えるル

ータとが普及するまでにはかなりの年月を要するという問題も抱えている。

【0017】

また、DDoS攻撃が発生している状態では通信の信頼性が保証できないため、上述した特許文献1に開示されている技術ではルータがプログラムを受信できない結果、攻撃元からのトラフィックが遮断されないという場合が考えられる。その一方で、特許文献1に開示されている技術ではルータ自体がDDoS攻撃の対象とされてしまう場合も考えられる。また、特許文献1に開示されている技術ではプログラムを増殖させる動作が行われるが、この動作が各組織のセキュリティポリシーに対する考え方とに染まないために採用が見送られる結果、DDoS攻撃に対して組織横断的に対処することができない場合も考えられる。

【0018】

また、前述した手法のうち、II. の手法においては、以下の問題が考えられる。

まず、攻撃対象顧客サイトによる対処技術では、ISPと攻撃対象顧客サイトとの境界で対策を実施するため、ISP内のネットワークの輻輳やルータ処理能力の低下には対処ができない。従って、DDoS攻撃がISPの他の顧客へ及ぼす影響を防ぐことができない。

【0019】

図15の例では、攻撃者によるISP-B3000を介したWebシステム1001へのDDoS攻撃を境界ルータ2001で対策すると、ISP-C4000を介してWebシステム1001へのアクセスを行っている正規利用者へのサービスの提供に影響を及ぼしてしまう。

【0020】

また、単一ISPによる対処技術では、ISPと隣接ISPとの境界で対策が実施されるため、自ISP内ネットワークへの影響は最小限となるが、隣接ISP内でのネットワークの輻輳やルータの処理能力の劣化には対処できないため、結果として隣接ISPから自ISPへ流入する正規のパケットが受ける影響を防ぐことができない。更にその上に、常時接続されているネットワーク境界のみでしか対策ができないため、時間と共に接続実体が変化する非常時接続ネットワークからの攻撃には正しく対処することができない。

【0021】

図15の例では、攻撃者によるISP-B3000を介したWebシステム1001へのDDoS攻撃を境界ルータ2002で対策すると、ISP-C4000を介してWebシステム1001へのアクセスを行っている正規利用者へのサービスの提供に及ぼす影響は少ないものの、ISP-B3000を介してWebシステム1001へのアクセスを行っている不図示の正規利用者へのサービスの提供にはやはり影響を及ぼしてしまう。しかも、図15の場合には、ISP-B3000が管理して

いるPOP境界ルータ3001に接続して攻撃を行っている攻撃者がPOP境界ルータ3001との接続を一旦断とした後に再度接続を行ったときには攻撃元のIPアドレスは変化してしまうため、ISP-A2000が管理している境界ルータ2002での対策は困難である。

【0022】

また、複数ISP連携による対処技術では、攻撃発信元により近い場所で対策を実施できるものの、現状ではISPの管理者が電話で相互に連絡を取り合ってお互いのセキュリティポリシーを尊重して問題に対処していく必要があるため、対策作業に相当の時間を要する。更にその上に、ISP担当者間の認証方法がないため、運用上の情報の信頼性、あるいはなりすましなどといったセキュリティの問題が生じる。また、ISP間で協調連携して対策した場合には作業履歴が残らないという問題も生じている。

【0023】

本発明は、このような従来の技術の問題点に鑑みてなされたものである。

すなわち、本発明が解決しようとする課題は、複数のISPが協調して不正アクセス発信元にできるだけ近い場所で不正アクセス対策を実施することにより、分散型サービス不能化攻撃に効果的に対処するための、不正アクセス着信拒否技術を提供することである。

【0024】

【課題を解決するための手段】

上述した課題を解決するための手段について図1を参照しながら説明する。

図1において、自ISP（インターネットサービスプロバイダ）10は自己の通信ネットワークであり、その運用は運用管理システム11によって管理されている。

【0025】

顧客サイト20のWebシステム21はWebサービスを自ISP10より公開しており、自ISP10によって管理されている顧客境界ルータ15にファイヤウォール22を介して接続されている。

【0026】

IDS（侵入検知システム）14は、顧客サイト20のWebシステム21への不正なアクセスを顧客境界ルータ15において検知し、検知された不正アクセスの内容を解析する。

【0027】

不正アクセスエージェントサイト13は不正アクセス通知手段13-1を必要に応じて備えており、IDS14から得られた情報を不正アクセス対策マネージャサイト12へ送付する。

【0028】

不正アクセス対策マネージャサイト12は、探索手段12-1、決定手段12-2、通知手段12-3、認証手段12-4、セキュリティポリシー交換手段12-

5、不正アクセス対策制御手段12-6、通知取得手段12-7、及び記録手段12-8を各々必要に応じて備えており、顧客サイト20のWebシステム21への不正なアクセスに対する対策を不正アクセス対策実施エージェントサイト16や18に指示する。

【0029】

不正アクセス対策実施エージェントサイト16は、トラフィックモニター手段16-1及び不正アクセス対策実施手段16-2をそれぞれ必要に応じて備えており、自

ISP10と論理的に隣接している通信ネットワークである隣接ISP30と自ISP10とを接続しているISP境界ルータ17において、顧客サイト20のWebシステム21への不正なアクセスに対する対策を行う。

【0030】

不正アクセス対策実施エージェントサイト18は、トラフィックモニター手段18-1及び不正アクセス対策実施手段18-2をそれぞれ必要に応じて備えており、自ISP10の利用者のうち常時接続を行わない者（非常時接続利用者）によって使用される非常時接続利用者端末40が自ISP10を利用するため接続するPOP（ポイント・オブ・プレゼンス）と自ISP10とを接続するPOP境界ルータ17において、顧客サイト20のWebシステム21への不正なアクセスに対する対策を行う。

【0031】

上述したように構成されている図1に示すシステムにおける不正アクセスマネージャサイト12、不正アクセス通知エージェントサイト13、並びに不正アクセス対策実施エージェントサイト16及び18が本発明に特に関係するものである。

【0032】

本発明に係る態様のひとつである不正アクセス対処システムは、自己の通信ネットワークより公開されているサービスに対する不正なアクセスの流入路の探索を行う探索手段12-1と、このサービスをこの不正なアクセスから保護するための対策を実施する場所の決定をこの探索の結果に基づいて行う決定手段12-2と、この不正なアクセスを自己の通信ネットワークに流入させている流入元でこの対策を実施するとの決定に応じて該決定を該流入元へ通知する通知手段12-3と、を有するよう構成することにより、前述した課題を解決する。

【0033】

この構成によれば、自己の通信ネットワーク（自ISP10）より公開されているサービス（Webシステム21によるWebサービス）に対する不正なアクセスへの対策を、自己の通信ネットワークにその不正なアクセスを流入させている流入元で実施するとの決定がその流入元へ通知されるので、その流入元、すなわち不正アクセスの発信元により近い場所で不正アクセスの対策の実施が可能となる結果、分散型サービス不能化攻撃に対する効

果的な対処が行えるようになる。

【0034】

なお、上述した本発明に係る不正アクセス対処システムにおいて、探索手段12-1は、前述した不正なアクセスが検知されたときに前述した探索を行うようにしてもよく、あるいは、不正なアクセスの検知がされたことが通知されたときに前述した探索を行うようにしてもよい。

【0035】

図1においては、不正なアクセスの検知はIDS14によって行われ、また、IDS14によって検知がされた不正なアクセスは不正アクセス通知手段13-1によって不正アクセス対策マネージャサイト12に通知される。

【0036】

こうすることにより、不正なアクセスに対して迅速な対策を行うことができるようになる。
また、前述した本発明に係る不正アクセス対処システムにおいて、探索手段12-1は、自己の通信ネットワークで伝送されているトラフィックの監視情報と前述した不正なアクセスの内容を示す不正アクセス情報に基づいて前述した流入路を探索するようにしてもよい。

【0037】

図1においては、自己の通信ネットワーク、すなわち自己のISP10で伝送されているトラフィックの監視情報は運用管理システム11より得られ、不正アクセス情報はIDS14により得られる。この不正アクセス情報により不正アクセスの特徴が判明するので、これと同様の特徴を有するトラフィックを監視情報から見つけ出すことにより、不正アクセスの流入路を判明させることができる。

【0038】

なお、ここで、監視情報は、自己の通信ネットワークと該自己の通信ネットワークに隣接する通信ネットワークとの境界に配置されている境界ルータの位置情報と、境界ルータを通過して自己の通信ネットワークへ流入したトラフィックについての監視情報を少なくとも含むものであってもよい。

【0039】

図1においては、境界ルータ（ISP境界ルータ17）の位置情報は運用管理システム11より得られ、境界ルータを通過して自己の通信ネットワークへ流入したトラフィックについての監視情報はトラフィックモニター手段16-1によって得られる。従って、これらの情報により、これと同様の特徴を有するトラフィックを監視情報から見つけ出すことにより、不正アクセス情報により示されている特徴を有する不正アクセスがどこから自己のISPに流入したのかを判明させることができる。

【0040】

なお、ここで、トラフィックモニター手段16-1は、

例えば、送信元アドレス、送信先アドレス、及び送信先ポート番号をキーとして、ISP境界ルータ17を介して流入するパケット数を単位時間毎且つ接続先毎に記録することにより、送信元アドレスが偽装されたパケットの流入路の把握が可能となる。

【0041】

また、トラフィックモニター手段18-1もトラフィックモニター手段16-1と同様の記録を行うことにより、POP境界ルータ19を介して流入する、非常時接続接続利用者端末40からの流入パケットを把握することができる。

【0042】

なお、好ましくは、トラフィックモニター手段16-1及び18-1は、運用管理システム11と連携して接続先情報を入手するうにしてもよい。
また、前述した本発明に係る不正アクセス対処システムにおいて、通知手段12-3は、前述した不正なアクセスの流入元との間で相互認証を行った後に前述した決定を該流入元へ通知するうにしてもよい。

【0043】

図1においては、この相互認証は認証手段12-4によって行われる。こうすることにより、流入元になりすました第三者による前述した決定の通知の窃取が防止される。

【0044】

ここで、この相互認証のための流入元との接続プロトコルは例えばHTTPs（Hypertext Transfer Protocol Security）プロトコルであってもよく、また、この相互認証で用いられる認証方式は例えば公開鍵基盤（PKI：Public Key Infrastructure）であってもよく、また電子証明書は例えばITU（国際電気通信連合）勧告X.509に則った形式であってもよい。

【0045】

また、前述した本発明に係る不正アクセス対処システムにおいて、通知手段12-3は、前述した不正なアクセスの流入元との間で各々のネットワーク運用におけるセキュリティポリシーに関する情報を交換した後に前述した決定を該流入元へ通知するうにしてもよい。

【0046】

図1においては、このセキュリティポリシーに関する情報の交換はセキュリティポリシー交換手段12-5によって行われる。こうすることにより、流入元とのセキュリティポリシーに違いが存在していても、その違いを調整した上で不正アクセスに対する対策を流入元に依頼することができるようになる。

【0047】

なお、ここで、セキュリティポリシーに関する情報として、データ暗号方式情報とタイムゾーンの情報との交換を行ってもよく、またデータ暗号方式の交換をするとき

信ネットワーク内で実施させる不正アクセス対策実施制御手段12-6を更に備えるようにしてよい。

【0048】

また、前記セキュリティポリシーに関する情報は、不正なアクセスが検知されなくなつてから該不正なアクセスに対する前記対策を解除するまでの時間を示す情報であつてもよい。

【0049】

こうすることにより、不正なアクセスが検知されなくなつてから該不正なアクセスに対する前記対策を解除するまでの時間についてのセキュリティポリシーに違いが存在していても、セキュリティポリシーに従つた対策を流入元に依頼することができる。

【0050】

また、このとき、セキュリティポリシーに関する情報によって示されている時間が自己のネットワークと流入元とで異なっているときには、両者のうち短い方の時間を、不正なアクセスが検知されなくなつてから該不正なアクセスに対する前記対策を解除するまでの時間とするようにしてよい。

【0051】

こうすることにより、自己のネットワークと流入元との両者で許容し得るセキュリティポリシーに従つた対策を流入元に依頼することができる。
また、このとき、通知手段12-3が、前述した決定と共に、不正なアクセスが検知されなくなつてから該不正なアクセスに対する前述した対策を解除するまでの時間を示す情報を流入元へ通知するようにしてよい。

【0052】

こうすることにより、自己のネットワークと流入元との両者で許容し得るセキュリティポリシーに従つたこの時間の設定が流入元に通知される。

また、前述した本発明に係る不正アクセス対処システムにおいて、通知手段12-3は、前述した不正なアクセスの流入路とは異なる通信経路を用いて前述した決定を該不正なアクセスの流入元へ通知するようにしてよい。

【0053】

不正なアクセスの流入路はDDoS攻撃の影響により通信路として利用できない場合があるので、こうすることにより、このような場合が発生していても前述した決定を流入元へ通知することができるようになる。

【0054】

また、前述した本発明に係る不正アクセス対処システムにおいて、通知手段12-3は、前述した自己の通信ネットワークに前述した不正なアクセスを流入させている流入元で前述した対策を実施する決定がされたときに、該決定を該流入元へ通知するか否かを判定し、この通知手段12-3によって前述した決定を該流入元へ通知しないとの判定がされたときに、前述したサービスを前述した不正なアクセスから保護するための対策を自己の通

なお、ここで、前述した判定が、予め与えられている前記流入元についての判定情報に基づいて行われるようにしてよい。

こうすることにより、例えば前述した決定を前述した流入先に通知しても前述した対策が該流入先で行ってもらえない場合であつても、このような不正アクセスに適切に対処することができるようになる。

【0056】

なお、ここでも、前述した判定が、予め与えられている前記流入元についての判定情報に基づいて行われるようにしてよい。

【0057】

こうすることにより、例えば前述した決定を前述した流入先に通知しても前述した対策が該流入先で行ってもらえないことが予め判明しているような場合にこのことを示す情報を予め判定情報として与えておくことにより、このような不正アクセスに適切に対処することができる。

【0058】

こうすることにより、不正アクセスの発信元が自己の通信ネットワーク（自ISP10）内より行われている場合に、自己の通信ネットワーク内でこのような不正アクセスに対する対策を適切に行わせることができるようにする。

【0059】

なお、図1において、例えば隣接ISP30から自ISPへWebシステム21への不正アクセスが流入している場合には、不正アクセス対策実施制御手段12-6は、ISP境界ルータ17で不正アクセスに対する対策の実施を不正アクセス対策実施エージェント16に指示する。不正アクセス対策実施エージェント16に設けられている不正アクセス対策実施手段16-2はこの指示に応じてISP境界ルータ17を制御し、隣接ISP30からのこの不正アクセスをISP境界ルータ17で遮断させる。

【0060】

なお、ここで、不正アクセス対策実施制御手段12-6は、前述した不正なアクセスの発信元が接続しているPOP（ポイント・オブ・プレゼンス）境界ルータにおいて前述した対策を実施するようにしてよい。

【0061】

図1において、例えば非常時接続利用者端末40がWebシステム21への不正アクセスの発信元である場合は、不正アクセス対策実施制御手段12-6は、POP

13

境界ルータ19で不正アクセスに対する対策の実施を不正アクセス対策実施エージェント18に指示する。不正アクセス対策実施エージェント18に設けられている不正アクセス対策実施手段18-2はこの指示に応じてPOP境界ルータ19を制御し、非常時接続利用者端末40からのこの不正アクセスをPOP境界ルータ19で遮断させる。

【0062】

なお、ここで、不正アクセス対策実施制御手段12-6は、前述した不正なアクセスの発信元が接続しているPOP境界ルータ19を、前述した自己の通信ネットワーク（自ISP10）の運用の管理を行っている運用管理システム11から得られる情報に基づいて特定するようにもよい。

【0063】

POP（ポイント・オブ・プレゼンス）接続においては、通信ネットワーク上で特定の端末を識別するために該端末に割り当てる識別子が接続の度に異なっていることが一般的である。従って、不正アクセスの発信元である非常時接続利用者端末40によってPOP接続が改めて行われるために異なる識別子がその非常時接続利用者端末40に割り当てられてしまい、その結果不正アクセスに対する適切な対策が取れなくなる場合がある。しかし、この割り当ては運用管理システム11によって管理されているので、この割り当て情報を利用することにより、POP接続が改めて行われて異なる識別子が割り当てられても、非常時接続利用者端末40からのこの不正アクセスをPOP境界ルータ19で適切に遮断させることができるようになる。

【0064】

また、自己の通信ネットワークとは異なる他の通信ネットワークより公開されているサービスに対する不正なアクセスを該他の通信ネットワークへ流入させている決定の通知を取得する通知取得手段12-7を更に有し、不正アクセス対策実施制御手段12-6は、通知取得手段12-7によって前述した通知が取得されたときには、上述した他の通信ネットワークより公開されているサービスを該通知に係る該不正なアクセスから保護するための対策を自己の通信ネットワーク内で実施せんようにしてもよい。

【0065】

こうすることにより、上述した他の通信ネットワークより公開されているサービスに対する不正なアクセスを該他の通信ネットワークに流入させている自己のネットワーク、すなわち不正アクセスの発信元により近い場所での不正なアクセスに対する適切な対策が実施される。

【0066】

また、不正アクセス対策実施制御手段12-6によって実施させた対策は、不正アクセスの検知がされなくなつたときから予め設定されている時間が経過した後には解

除されるようにしてよい。

【0067】

ここで、この予め設定されている時間は、自己の通信ネットワークと前述した他の通信ネットワークとの各々のネットワーク運用におけるセキュリティポリシーに基づいて設定されているようにしてよい。

【0068】

こうすることにより、不正アクセスについての対策によって正規のアクセス受けてしまう影響が、不正アクセスが停止してから所定の時間が経過した後には解消されるようになる。

【0069】

なお、このとき、自己の通信ネットワークと前述した他の通信ネットワークとの各々のネットワーク運用におけるセキュリティポリシーに基づいて設定されている時間が両者間で異なっているときには、不正アクセスの検知がされなくなったときから両者のうち短い方の時間が経過した後には解除されるようにしてよい。

【0070】

こうすることにより、不正アクセスについての対策によって正規のアクセス受けてしまう影響が解消されるまでの時間が、自己の通信ネットワークと他の通信ネットワークとの両者で許容し得るセキュリティポリシーに従った時間となる。

【0071】

また、前述した本発明に係る不正アクセス対処システムにおいて、自己の通信ネットワークとは異なる他の通信ネットワークより公開されているサービスに対する不正なアクセスを該他の通信ネットワークへ流入させている

30 決定の通知を取得する通知取得手段12-7を更に有し、探索手段12-1は、通知取得手段12-7によって前述した通知が取得されたときには、該通知に係る不正なアクセスの自己の通信ネットワークにおける流入路を探索し、決定手段12-2は、通知取得手段12-7によって前述した通知が取得されたときには、前述した他の通信ネットワークより公開されているサービスを該通知に係る不正なアクセスから保護するための対策を実施する場所を前述した探索の結果に基づいて決定し、通知手段12-3は、通知取得手段12-7によって前述した通知が取得されたときには、該通知に係る不正なアクセスを自己の通信ネットワークに流入させている流入元で前述した対策を実施する決定に応じて該決定を該流入元へ通知するようにしてよい。

【0072】

こうすることにより、上述した他の通信ネットワークより公開されているサービスに対する不正なアクセスを自己の通信ネットワークに流入させている更に上流の流入元、すなわち不正アクセスの発信元に更に近い場所での不正なアクセスに対する適切な対策が実施される。

50 【0073】

なお、このとき、通知取得手段12-7によって取得された通知が過去に取得されたものと同一の通知であるときに、自己の通信ネットワーク若しくは前述した他の通信ネットワークより公開されているサービスを該通知に係る不正なアクセスから保護するための対策を該通知の通知元の通信ネットワーク内で実施させる不正アクセス対策実施制御手段12-6を更に有するように構成してもよい。

【0074】

通知取得手段12-7によって取得された通知が過去に取得されたものと同一の通知であるときには、その後も通知が繰り返されるだけで不正アクセスに対する対策が全くなされてないおそれがあると見ることができる。上述した構成によれば、このような場合にも不正アクセスに対する対策が適切に実施される。

【0075】

なお、このとき、通知手段12-3は、前記決定を通知するときに該通知に係る不正なアクセスを一意に特定する情報を併せて通知するようにしてもよい。こうすることにより、不正アクセス対策実施制御手段12-6は、通知取得手段12-7によって取得された通知が自己の通知手段12-3による通知に起因して通知されていたものであるかどうかを、該通知に含まれている該通知に係る不正なアクセスを一意に特定する情報に基づいて判定することができる。

【0076】

また、前述した本発明に係る不正アクセス対処システムにおいて、通知手段12-3による通知の履歴を記録する記録手段12-8を更に有するように構成してもよい。

【0077】

この構成によれば、自己の通信ネットワーク（自ISP10）の管理者が流入元へ行った不正アクセスへの対処の依頼の状況をこの履歴の記録から把握することができるようになる。

【0078】

なお、上述した本発明に係る不正アクセス対処システムの各構成により行なわれる機能と同様の処理をコンピュータに行わせるプログラムであっても、そのプログラムをコンピュータに実行させることによって本発明に係る不正アクセス対処システムと同様の作用・効果が得られるので、前述した課題を解決することができる。

【0079】

また、上述した本発明に係る不正アクセス対処システムの各構成により行なわれる手順からなる方法であっても、その方法を使用することによって本発明に係る不正アクセス対処システムと同様の作用・効果が得られるので、前述した課題を解決することができる。

【0080】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。図2は本発明を実施する不正アクセス対処システムの機能構成を示している。このシステムは、不正アクセス対策マネージャサイト100、不正アクセス通知エージェントサイト200、及び不正アクセス対策実施エージェントサイト300が不正アクセス対処システム専用ネットワーク400で接続されて構成されており、自己の通信ネットワークであるISPネットワーク500内に構築されている。また、このシステムは運用管理システム501及び不正アクセスの検知を行うIDS（Intrusion Detection System）502と連携することによって機能する。

【0081】

不正アクセス対策マネージャサイト100は不正アクセス対策マネージャプログラム110を実行するコンピュータである。不正アクセス対策マネージャサイト100は2つの通信インターフェースを有しており、その一方はISPネットワーク500に接続され、他方は不正アクセス対処システム専用ネットワーク400に接続されている。但し、2つのネットワーク間のルーティングは行わない。

【0082】

不正アクセス対策マネージャプログラム110が実行されると不正アクセス対策制御部111、不正アクセス対策記録制御部112、及びIO制御部113が構成される。

【0083】

不正アクセス対策制御部111は不正アクセス対策実施場所決定、組織間認証、及び組織間ポリシー交換の各機能を呼び出し、各機能の実行順序を制御する。

不正アクセス対策記録制御部112は不正アクセスに対してこの不正アクセス対処システムによって行われた対策内容の履歴の記録を制御する。

【0084】

IO制御部113は、ISPネットワーク500及び不正アクセス対処システム専用ネットワーク400での通信の制御、及び不正アクセス対策マネージャサイト100に設けられているDB（データベース）に対するデータ操作の制御を行う。

【0085】

証明書120は不正アクセス対策制御部111の制御によって組織間認証が行われるときに使用されるものであり、例えばITU（国際電気通信連合）勧告X.509に則った形式のものである。

【0086】

Policy（ポリシー）130はISPネットワーク500のセキュリティポリシーが示されている情報ファイルである。

Log（ログ）DB140は不正アクセスに対してこの不正アクセス対処システムによって行われた対策内容の

履歴が記録されるデータベースである。

【0087】

管理端末101はこの不正アクセス拒否システムのためのユーザインターフェースをISPネットワーク500の管理者に提供するものであり、CPU、メモリ、ディスプレイ、通信インターフェース等を有するコンピュータである。なお、管理端末101としては例えばパーソナルコンピュータや携帯情報端末(PDA)等が利用可能である。

【0088】

不正アクセス通知エージェントサイト200は不正アクセス通知プログラム210を実行するコンピュータである。不正アクセス通知エージェントサイト200は2つの通信インターフェースを有し、その一方はISPネットワーク500に接続され、他方は不正アクセス対処システム専用ネットワーク400に接続されている。但し、この2つのネットワーク間のルーティングは行わない。

【0089】

不正アクセス通知プログラム210が実行されると不正アクセス通知エンジン211と通信制御部212とが構成される。

不正アクセス通知エンジン211はIDS502によって検知された不正アクセスに関する情報をIDS502から取得して不正アクセス対策マネージャサイト100に通知する制御を行う。

【0090】

通信制御部212はISPネットワーク500及び不正アクセス対処システム専用ネットワーク400での通信の制御を行う。

不正アクセス対策実施エージェントサイト300は不正アクセス対策実施エージェントプログラム310を実行するコンピュータである。不正アクセス対策実施エージェントサイト300は2つの通信インターフェースを有しており、その一方はISPネットワーク500に接続され、他方は不正アクセス対処システム専用ネットワーク400に接続されている。但し、2つのネットワーク間のルーティングは行わない。

【0091】

不正アクセス対策実施プログラム310が実行されると不正アクセス対策実施エンジン311、トラフィックモニターエンジン312、及びIO制御部313が構成される。

【0092】

不正アクセス対策実施エンジン311は不正アクセス対策マネージャサイト100から送られてくる情報に基づいて境界ルータ503を制御して不正アクセスを遮断させる。

【0093】

トラフィックモニターエンジン312は境界ルータ503に流入するトラフィックを監視して監視情報を記録す

る制御を行う。

IO制御部313は、ISPネットワーク500及び不正アクセス対処システム専用ネットワーク400での通信の制御、及び不正アクセス対策実施エージェントサイト300に設けられているDB(データベース)に対するデータ操作の制御を行う。

【0094】

トラフィックDB320は境界ルータ503に流入したトラフィックの情報が記録されるデータベースである。

- 10 運用管理システム501はISPネットワーク500内に配置されてISPネットワーク500の運用の管理を行うシステムであり、ISPネットワーク500の構成管理、トラフィック管理、障害管理、アカウント管理等を行っている。運用管理システム501は不正アクセス対策マネージャサイト100と連携し、各種のデータの受け渡しを行う。

【0095】

IDSシステム502は、ISPネットワーク500と顧客によって運用されている顧客ネットワークとの境界

- 20 の好ましくはISPネットワーク500側に配置され、悪意ある発信元からの不正アクセスの検知を行っている。IDSシステム502は不正アクセス通知エージェントサイト200と連携し、各種のデータの受け渡しを行う。

【0096】

境界ルータ503はISPネットワーク500と論理的に隣接している他の通信ネットワーク(隣接ネットワーク)の境界に設置されているルータ、あるいはISPネットワーク500の利用者のうち常時接続を行わない者

- 30 (非常時接続利用者)によって使用される非常時接続利用者端末がISPネットワーク500を利用するためには接続するPOP(ポイント・オブ・プレゼンス)とISPネットワーク500との境界に設置されているルータである。境界ルータ503は不正アクセス対策実施エージェントサイト300と連携し、各種のデータの受け渡しを行う。なお、図2には境界ルータ503がISPネットワーク500に一台だけ設置されているように描かれているが、ここでは複数台の境界ルータ503がISPネットワーク500に設置されているものとする。

【0097】

- 40 不正アクセス対処システム専用ネットワーク400は、ISPネットワーク500とは別の通信ネットワークである。不正アクセス対処システム専用ネットワーク400にはISPネットワーク500に設けられている不正アクセス対処システムが接続されていることに加え、隣接ネットワークに設けられている図2と同様の構成の不正アクセス対処システムも接続されており、各種のデータの受け渡しが行われる。なお、これらの機器間での各種のデータの授受は原則としてこの不正アクセス対処システム専用ネットワーク400を介して行われる。

【0098】

なお、図2に示した不正アクセス対策マネージャサイト100、不正アクセス通知エージェントサイト200、及び不正アクセス対策実施工エージェントサイト300は、いずれも例えば図3に示すようなハードウェア構成を有するコンピュータを用いて構成することができる。

【0099】

図3について説明する。

同図に示すコンピュータはCPU601、RAM602、ROM603、HDD604、入力部605、出力部606、通信インターフェースA607、及び通信インターフェースB608がバス609を介して相互に接続されて構成されており、CPU601による管理の下で相互にデータ授受を行うことができる。

【0100】

CPU(Central Processing Unit)601はこのコンピュータ全体の動作制御を司る中央処理装置である。

RAM(Random Access Memory)602は、各種の制御プログラムをCPU601が実行するときにワークメモリとして使用され、また各種のデータの一時的な格納領域として必要に応じて用いられるメインメモリとしても使用されるメモリである。

【0101】

ROM(Read Only Memory)603はCPU601によって実行される基本制御プログラムが予め格納されているメモリであり、このコンピュータの起動時にCPU601がこの基本制御プログラムを実行することによってこのコンピュータ全体の動作の基本的な制御がCPU601によって行えるようになる。

【0102】

HDD(Hard Disk Drive)604は、各種のデータを記録しておくデータベースとして利用されるハードディスク装置である。また、HDD604にはCPU601によって実行される各種の制御プログラムが予め格納されている。

【0103】

入力部605は外部からの入力を受け取ってその入力の内容をCPU601に渡すものであり、必要に応じ、例えればキーボードやマウスなどといったこのコンピュータを操作する操作者からの指示を受け取る入力装置、あるいはFD(Flexible Disk)、CD-ROM(Compact Disc-ROM)、DVD-ROM(Digital Versatile Disc-ROM)、MO(Magneto-Optics)ディスクなどといった可搬型の記録媒体の読出装置を備えて構成される。

【0104】

出力部606はCPU601からの指示に応じた出力を行うものであり、例えば各種データを表示するCRT

(Cathode Ray Tube)やLCD(Liquid Crystal Display)を備えて構成される表示装置や各種データを印刷して表示するプリンタ装置などである。

【0105】

なお、このコンピュータを不正アクセスマネージャサイト100として使用する場合には、管理端末101を入力部605や出力部606として利用してもよい。

【0106】

10 通信インターフェースA607は、このコンピュータをISPネットワーク500に接続して他のシステムとの間でのデータ授受を行う際の通信管理を行うものである。

【0107】

通信インターフェースB608は、このコンピュータを不正アクセス対処システム専用ネットワーク400に接続してISPネットワーク500に設けられている不正アクセス対処システムを構成する他のサイトとの間、あるいは隣接ネットワークに設けられている不正アクセス対処システムとの間でデータ授受を行う際の通信管理を行うものである。

【0108】

図3に示すコンピュータは以上の各構成要素を備えて構成される。

以下、図2に示した不正アクセス対処システムを構成する各サイトで前述した各種のプログラムを実行することによって構成される各部によって行われる処理の内容について説明する。

【0109】

30 なお、図2に示した不正アクセス対処システムでは、これより説明するトラフィックモニター手順、不正アクセス通知手順、不正アクセス対策制御手順、不正アクセス対策記録手順が並行して行われる。

【0110】

まず図4について説明する。同図はトラフィックモニターエンジン312によって行われるトラフィックモニタ一手順の内容をフローチャートで示したものである。

【0111】

40 まず、S101においてスレッドの分岐が行われ、その一方ではS102の繰り返し手順が、他方ではS103からS105にかけての繰り返しの手順が、それぞれ実行される。

【0112】

S102では、境界ルータ503へ流入しているトラフィックであるIP(Internet Protocol)パケット(以下、単に「パケット」と称することとする)がキャプチャー(捕獲)される。以降、S102の手順が繰り返されて境界ルータ503に流入するパケットが全てキャプチャーされる。

【0113】

50 S103では、S103からS105にかけてのスレッ

21

ドの実行が一定の時刻レンジだけ、例えば10分間だけスリープ（停止）され、その後、所定の時刻レンジが経過したときにS104の手順に進む。

【0114】

S104では、S102の処理によってキャプチャーされているパケットの数が、接続ID、時刻レンジ、SrcIP、DistIP、及びDistPortをキーにして計数され、続くS105においてその計数の結果を示すデータが監視情報としてトラフィックDB320に格納される。このS105の手順が完了した後にはS103へ手順を戻して上述した手順が繰り返される。

【0115】

ここで図5について説明する。同図は上述したS105の手順によってデータの格納が行われるトラフィックDB320のデータ構造を示している。同図に示すように、トラフィックDB320にはレコード毎に「接続ID」、「時刻レンジ」、「SrcIP」、「DistIP」、「DistPort」、及び「Count」の各フィールドが設けられている。

【0116】

接続IDは、ISPネットワーク500の利用者に個別に割り当てられている識別子である。接続IDと計数対象とするパケットとの関係は、そのパケットに示されているSrcIPを運用管理システム501に送付して問い合わせを行うことによって運用管理システム501から得ることができる。

【0117】

時刻レンジはパケットの計数の開始時刻及び終了時刻の組である。

SrcIPは計数対象とするパケットに示されている送信元のIPアドレスである。

【0118】

DistIPは計数対象とするパケットに示されている宛先のIPアドレスである。

DistPortは計数対象とするパケットに示されている宛先のポート番号である。

【0119】

Countは「時刻レンジ」に示されている時間内に境界ルータ503に流入した計数対象とするパケットの数である。

図5に示されているデータ例のうち第一行目のレコードについて解説すると、接続IDとして「ABC01234」が割り当てられているISPネットワーク500の利用者は、「10:00-10:10」の時間内に、送信元のIPアドレスが「202.248.20.254」、宛先のIPアドレスが「202.248.20.68」、そして宛先のポート番号が「80」である「1456」個のパケットを境界ルータ503に流入させたことを示している。

【0120】

22

なお、トラフィックDB320には上述したデータが境界ルータ503毎に格納される。

以上のトラフィックモニター手順が行われることによって、境界ルータ503に流入するパケットの監視が行われる。

【0121】

次に図6について説明する。同図は不正アクセス通知エンジン211によって行なわれる不正アクセス通知手順の内容をフローチャートで示したものである。

10 まず、S201において、IDS502の不正アクセスイベントのチェックが行われ、続くS202において不正アクセスの検知がIDS502によってなされたか否かが判定される。この結果、不正アクセスの検知がされたと判定された（判定結果がYes）ならばS203に手順を進め、不正アクセスの検知がされていないと判定された（判定結果がNo）ならばS201へ手順を戻して上述した手順が繰り返される。

【0122】

S203では、検知された不正アクセスについての通知が不正アクセス対策マネージャサイト100の不正アクセス対策制御部111へ行われる。その後はS201へ手順を戻して上述した手順が繰り返される。

【0123】

ここで図7について説明する。同図は上述したS203の手順によって不正アクセス対策制御部111へ行われる不正アクセスの通知のデータ形式を示している。同図に示すように、この不正アクセス通知には、「検知ID」、「時刻レンジ・スタート」、「時刻レンジ・エンド」、「攻撃種別」、「組織名」、「所属ISP」、30 「ターゲットプロトコル」、「SrcIP」、「DistPort」、「不正パケット数」、「攻撃ツール名」、「対策解除ポリシー」の各情報が含まれている。なお、これらのデータはIDS502から得ることができる。

【0124】

検知IDは、不正アクセスの検知がなされる度にIDS502によってその不正アクセスに対して付与される一意な識別子であり、この検知IDによってDDoS攻撃を個別に特定する指標とすることができる。

40 【0125】

時刻レンジ・スタート及び時刻レンジ・エンドは、それぞれ不正アクセスに係るパケットが最初に検知された日時及びこの日時から所定の時間（例えば10分間）が経過したときの日時であり、図7の例ではこれらの日時がグリニッジ標準時(GMT)で示されている。

【0126】

攻撃種別は、検知された不正アクセスであるDDoS攻撃の詳細種別である。

組織名は、不正アクセスを受けているシステムが属して50 いる組織の組織名である。

【0127】

所属ISPは、不正アクセスを受けているシステムが属している組織が所属しているISPの名称である。ターゲットプロトコルは不正アクセスが攻撃を受けているシステムへの接続に利用しているプロトコルである。

【0128】

SrcIPは不正アクセスに係るパケットに示されている送信元のIPアドレスである。
DstIPは不正アクセスに係るパケットに示されている宛先のIPアドレスである。

【0129】

DstPortは不正アクセスに係るパケットに示されている宛先のポート番号である。
不正パケット数は検知IDで特定される不正アクセスに係るパケットの数である。

【0130】

攻撃ツール名は、不正アクセスに使用されているDDoS攻撃ツールのツール名である。
対策解除ポリシーは、この不正アクセスが停止してからこの対策を解除するまでの時間である。この時間はISPネットワーク500におけるセキュリティポリシーで許容される範囲内で例えば不正アクセスを受けている顧客からの指示により予め設定される。

【0131】

図7に示されているデータ例のうちの例1の不正について解説すると、IDS502によって検知された「00-00-0E-82-2E-74-001」なる検知IDで特定される不正アクセスは、「2003/2/1・16:01:16」から検知された「TCP SYN Flood」攻撃であり、この攻撃は「ISP AB C」に属する「Company A」への「TCP」プロトコルによるものであって、攻撃元は「TFN2K」なる攻撃ツールを使用しており、送信元のIPアドレスが「10.4.120.2」、宛先のIPアドレスが「192.168.X.Y」、宛先のポート番号が「80」であるパケットが「2003/2/1・16:11:16」までの間に「156789」個送りつけられてきたこと、この不正アクセスについての対策は当該不正アクセスが停止してからも「10分間」は継続して実施すべきことを示している。

【0132】

以上の不正アクセス通知手順が行われることによって、IDS502による顧客ネットワークへの不正アクセスの検知の内容が不正アクセス対策マネージャサイト100の不正アクセス対策制御部111へ通知される。

【0133】

次に図8について説明する。同図は不正アクセス対策制御部111によって行われる不正アクセス対策制御手順の内容をフローチャートで示したものである。

まず、S301において、不正アクセス通知エージェン

トサイト200からの不正アクセスの通知をひとつ取り出す。

【0134】

S302では、この取り出された不正アクセス通知に示されている前述した検知IDが参照され、この検出IDが過去に取得していた不正アクセス通知に示されていたか否か、より具体的にはこの検知IDと同一のものがLogDB140に記録されているか否かが判定される。そして、この判定結果がYesならばS314に手順が進み、NoならばS303に手順が進む。

【0135】

S303では不正アクセス対策実施場所決定手順が実行される。この手順の詳細は図9にフローチャートで示されている。

以下、この図9の手順を先に説明する。

【0136】

まず、S321において、運用管理システム501に対する問い合わせが行われて、ISPネットワーク500に設置されている境界ルータ503の一覧が取得される。

【0137】

S322では、不正アクセス対策実施エージェントサイト300に対する問い合わせが行われ、図8のS301の手順において取り出された不正アクセス通知に示されていた、時刻レンジ、SrcIP、DstIP、及びDstPortの一一致しているレコードをトラフィックDB320から抽出する。そして、その抽出されたレコードに示されていたトラフィックが流入していた境界ルータ503を残してそのほかの境界ルータ503を前の手順で取得されていた境界ルータ503の一覧から除外する。

【0138】

S323では、先の一覧に残されている境界ルータ503から非常時接続利用者用端末のために設けられているもの（非常時接続境界ルータ）が抽出され、抽出された非常時接続境界ルータについてのトラフィックIDB320の格納データから、前述した不正アクセス通知に関係しているデータレコードに示されている接続IDが取得される。

【0139】

S324では、前の手順で取得された接続IDで特定される利用者がISPネットワーク500に現在接続しているかどうかの問い合わせが運用管理システム501へ行われる。そして、この利用者がISPネットワーク500に現在接続しているのであればこの利用者によって現在使用されている非常時接続利用者端末からのパケットが流入している非常時接続境界ルータを抽出して先の一覧に残し、一方、この利用者が現在はISPネットワーク500に接続していないのであれば、この利用者によって使用されていた非常時接続利用者端末からの不正

アクセスを流入させていた非常時接続境界ルータを先の一覧から除外する。

【0140】

S325では、一覧に残されている境界ルータ503の各々の接続先に基づいて、先の通知に係る不正アクセスについての対策を自組織で実施するか、あるいはこの対策の実施を他組織に依頼するかを分類する。

【0141】

この分類の基準は、より具体的には、一覧に残されている境界ルータ503が非常時接続境界ルータであるか、あるいはISPネットワーク500とは信頼関係のない隣接ISPとの境界に設置されているISP境界ルータであるならば、この境界ルータ503において自組織でこの対策を実施するものとする。一方、一覧に残されている境界ルータ503がISPネットワーク500と信頼関係にある隣接ISPとの境界に設置されているISP境界ルータであるならば、このISP境界ルータでは対策を行わずにその隣接ISPにこの対策の実施を依頼するものとする。この手順によって前述した通知に係る不正アクセスについての対策を実施する場所が全て決定される。

【0142】

S325の手順を終えた後には図8の手順へ戻る。

図8のS304では、上述した不正アクセス対策実施場所決定手順で求めた、対策実施場所が取り出される。

【0143】

S305では、S304の手順で取り出された対策実施場所のうち、未対策のまま残されている場所の数が0よりも大きいか否かが判定され、この判定結果がYes、すなわち未対策の場所が残されているのであればS306に手順を進める。一方、この判定結果がNo、すなわち対策を実施すべき全ての場所での対策が完了したならばS301へ手順を戻して上述した手順が繰り返される。

【0144】

S306では、S304の手順で取り出された対策実施場所のうち、未対策のまま残されている場所が一つ取り出される。

S307では、前の手順で取り出された場所が、自組織でこの対策を実施するとしている境界ルータ503であるか否かが判定され、この判定結果がYesならばS308に手順を進める。一方、この判定結果がNo、すなわちこの場所がその隣接ISPにこの対策の実施を依頼するものとしたISP境界ルータであったならばS309に手順を進める。

【0145】

S308では、前の手順で取り出された場所である境界ルータ503を制御する不正アクセス対策実施エージェントサイト300に対して不正アクセス対策実施要求が送付され、その後はS312に手順が進む。

【0146】

この不正アクセス対策実施要求には対策を実施させる境界ルータ503を特定する情報が示されており、更にS301の処理で取り出されていた不正アクセス通知が添付されている。この要求を受け取った不正アクセス対策実施エージェントサイト300では、不正アクセス対策実施エンジン311によって不正アクセス対策実施手順が実行される。

【0147】

10 不正アクセス対策実施手順の詳細は図10にフローチャートで示されている。以下、この図10の手順を先に説明する。

まず、S401において、不正アクセス対策マネージャサイト100から送られてきた不正アクセス対策実施要求が取得される。

【0148】

S402では、運用管理システム501に対する問い合わせが行われ、運用管理システム501から送られてくる不正アクセス対策実施要求に示されていた境界ルータ503を制御するために必要な固有情報、例えばこの境界ルータ503の機器種別、機器管理のための管理者ID及びパスワード等が取得される。

【0149】

S403では、前の手順によって取得された固有情報を使用して境界ルータ503が制御され、不正アクセス対策実施要求に添付されていた不正アクセス通知に含まれるSrcIP、DstIP、DstPort、攻撃種別情報に基づいて、この通知に係る不正アクセスと同一のパケットの通過を遮断するフィルタを境界ルータ503が設定される。

【0150】

S404ではスレットの分岐が行われ、その一方ではS401からS403にかけての繰り返しの手順が実行され、他方ではS405からS408にかけての手順が実行される。

【0151】

S405では、前述したS403の手順で設定したフィルタの状況が境界ルータ503から取り出される。

S406では、前のステップで取り出されたフィルタの状況から、対策解除時間閾値を超えて不正アクセスであるパケットが継続して境界ルータ503に到来していないかどうかが判定され、この判定結果がYes、すなわち対策解除時間閾値を超えて不正アクセスであるパケットが継続して到来していないのであればS407に手順を進め、一方、この判定結果がNo、すなわち不正アクセスであるパケットが依然として到来しているかあるいは不正アクセスであるパケットが到来していない継続時間が対策解除時間閾値に未だ満たないときにはS405へ手順を戻して上述した手順が繰り返される。なお、対策解除時間閾値については後述する。

【0152】

S407では、境界ルータ503が制御されて前述したS403の手順で設定したフィルタが解除される。S408では、不正アクセス対策マネージャサイト100の不正アクセス対策記録制御部112へログ要求が送付され、対策の実施完了の記録の依頼が行われる。なお、このログ要求には、S301の手順によって取得された不正アクセス通知が添付される。

【0153】

S408の手順を終えた後にはS404の手順によって分岐させたS405からS408にかけてのスレッドを終了させる。以上の不正アクセス対策実施手順が行われることによって、不正なアクセスへの対策が実施されて顧客ネットワークが不正なアクセスから保護される。

【0154】

図8の手順の説明へ戻る。

前述したS307の手順における判定の結果がNoであったとき、すなわち前述したS306の手順において取り出された場所が、不正アクセスについての対策の実施を隣接ISPに依頼するものとしたISP境界ルータであったときにはS309において組織間認証手順が実行される。この手順の詳細は図11にフローチャートで示されている。

【0155】

以下、この図11の手順を先に説明する。

まず、S331においてサーバ認証処理が証明書120を用いて行われ、対策の依頼先である隣接ISP（サーバ）が確かに信頼関係にあるISPであって悪意あるサイトのなりすましでないことを確認が行われる。

【0156】

続くS332ではクライアント認証処理が証明書120を用いて行われ、対策依頼元であるISPネットワーク500（クライアント）が確かに信頼関係にあるISPで、悪意あるサイトのなりすましでないことを確認が対策の依頼先であるISPで行われる。

【0157】

このS332の手順が終了したときには図8の手順へ戻る。

以上の組織間認証手順が行われることによって、不正アクセス対策に関する情報の悪意あるサイトによるなりすましでの窃取が防止される。

【0158】

図8においてS309に続いて行われるS310では組織間ポリシー交換手順が実行される。この手順の詳細は図12にフローチャートで示されている。

以下、この図12の手順を先に説明する。

【0159】

まず、S341において、第三者による情報の解読を不可能にするために、対策依頼元であるISPネットワー

ク500と対策依頼先である隣接ISPとの間で暗号アルゴリズムの交換が行われる。

【0160】

S342では、対策依頼元であるISPネットワーク500と対策依頼先である隣接ISPとの間で自己の対策解除時間閾値の交換が行われ、そのうちの短いものが両者間での対策解除時間閾値として採用される。

【0161】

ここで対策解除時間閾値について説明する。

- 10 対策解除時間閾値とは、ある不正アクセスが検知されなくなってから後にどの程度の時間までその不正アクセスに対する対策を継続するかを示す閾値である。この閾値は自己のネットワーク運用におけるセキュリティポリシーに従って各ISPで独自に設定されるが、ISP間で異なる値が設定されている場合には、本実施形態においてはそのうちのより短い時間を示している閾値を、その両者によって伝送されている不正アクセスに対して採用することとする。これは、閾値を長時間とすればそれだけ不正アクセスではない正規のアクセスも遮断してしまうおそれがあることからである。

【0162】

従って、例えばPolicy130に示されている対策依頼元の対策解除時間閾値が10分に設定されており、一方、対策依頼先の対策解除時間閾値が20分に設定されている場合には、その両者によって伝送されている不正アクセスについての対策解除時間閾値としては10分が採用されることになる。

【0163】

- 30 なお、このようにして決定された対策解除時間閾値よりも、前述した不正アクセス通知に示されていた対策解除ポリシーの値の方がより短い時間を示していたときには、顧客の指示に従うため、この対策解除ポリシーの値を対策解除時間閾値として採用する。

【0164】

- 40 S343では、対策依頼元であるISPネットワーク500と対策依頼先である隣接ISPとの間でタイムゾーン（地域別時間帯情報）の交換が行われる。これは、双方で対策内容の記録を行うときの時刻情報をローカル時間で表わすことを可能にして利便性を向上させる等の用途のために行われるものである。

【0165】

- このS343の手順が終了したときには図8の手順へ戻る。

- 以上の組織間ポリシー交換手順が行われることによって、ネットワーク運用に関するセキュリティポリシーに組織間で違いが存在していても、その違いを調整した上で不正アクセスに対する対策を依頼先に実施してもらうことができるようになる。

50 【0166】

図8においてS310に続いて行われるS311では、前述したS301の手順において取り出された不正アクセス通知が、対策依頼先である隣接ISPへ転送される。なお、このとき、S301の手順において取り出された不正アクセス通知に示されている対策解除ポリシーの値と、前述した組織間ポリシー交換手順の実行によって採用された対策解除時間閾値とが異なっているときには、このときの対策解除時間閾値を対策解除ポリシーの値として上書きした上で対策依頼先である隣接ISPへ転送するようになる。

【0167】

S312では不正アクセス対策記録制御部112へログ要求が送付され、上述したS308の手順またはS309からS311にかけての手順で行われた処理の内容の記録の依頼が行われる。なお、このログ要求には、S301の手順によって取得された不正アクセス通知が添付される。

【0168】

S313では、S303の不正アクセス対策実施場所決定手順で求めた対策実施場所数を1減らし、その後はS305へ手順を戻して上述した処理が繰り返される。

【0169】

ところで、前述したS302の手順における判定の結果がYesであったときには、その後も不正アクセス通知の転送がISP間で繰り返される（不正アクセス通知がループしている）だけで不正アクセスに対する対策が全くなされてないおそれがあると見ることができる。

【0170】

そこで、この場合には、まず、S314において、不正アクセス対策記録制御部112へログ要求が送付され、ループしている不正アクセス通知を取得した旨の記録の依頼が行われる。なお、このログ要求には、S301の手順によって取得された不正アクセス通知が添付される。

【0171】

その後は、S315において、S301で取り出された不正アクセス通知を送付してきた通知元（すなわち不正アクセス対策依頼の依頼元）のISPの不正アクセス対策マネージャサイト100に指示を与えて、そこで実行されている不正アクセス対策制御手順をS308から開始させることにより、この不正アクセス通知に係る不正アクセスに対する対策をそのISP内で実施せらるようになる。

【0172】

以上の不正アクセス対策制御手順が行われることによって、不正なアクセスへの対策の実施が指示されて顧客ネットワークが不正なアクセスから保護される。

次に図13について説明する。同図は不正アクセス対策記録制御部112によって行われる不正アクセス対策記録手順の内容をフローチャートで示したものである。

【0173】

まず、S501において、不正アクセス対策制御部111や不正アクセス対策実施エージェントサイト300の不正アクセス対策実施エンジン311から送られてくるログ要求が取り出される。

【0174】

S502では、取り出されたログ要求に基づいて、時刻、アクション、検出ID、時刻レンジ、SrcIP、DstIP、DstPort、不正パケット数、攻撃種別をログに記録してLogFile140に格納する。なお、ここで、「アクション」とは、例えば対策の実施、対策の転送（隣接ISPへの対策の依頼）、対策の解除、あるいは対策の中止など、どのような処置が実行されたときにログの記録が要求されたかを示す情報である。

【0175】

このS502の手順を終えた後にはS501へと手順を戻し、以降は上述したログ要求の取り出しとログへの記録の手順が繰り返される。

20 以上の大不正アクセス対策記録手順が行われることにより、ISPネットワーク500の管理者は顧客ネットワークに対する不正アクセスへの対処の状況をこの履歴の記録から把握することができるようになる。

【0176】

なお、図2は本発明を実施する不正アクセス対処システムの各構成要素によって実行される各種の制御プログラムをコンピュータで読み取り可能な記録媒体に記録させ、その制御プログラムを記録媒体からコンピュータに読み出させて実行することによって本発明を実施するようにもよい。

【0177】

記録させた制御プログラムをコンピュータで読み取ることの可能な記録媒体の例を図14に示す。このような記録媒体としては、データやプログラム等の情報を電気的、磁気的、光学的、機械的、または化学作用によって蓄積し、コンピュータから読み取ることができるものであればよく、このような記録媒体としては、同図に示すように、例えば、コンピュータ701に内蔵若しくは外付けの付属装置として備えられるRAM若しくはROM又はハードディスク装置などのメモリ702、あるいはフレキシブルディスク、MO（光磁気ディスク）、CD-ROM、CD-R/W、DVD、8mmテープ、メモリカードなどといった可搬型記録媒体703等が利用できる。

【0178】

また、記録媒体は通信回線704を介してコンピュータ701と接続される、プログラムサーバ705として機能するコンピュータが備えている記憶装置706であってもよい。この場合には、制御プログラムを表現するデータ信号で搬送波を変調して得られる伝送信号を、プロ

31

グラムサーバ45から伝送媒体である通信回線704を通じて伝送するようにし、コンピュータ701では受信した伝送信号を復調して制御プログラムを再生することで当該制御プログラムを実行できるようになる。

【0179】

ここで、伝送媒体としては、有線通信媒体、例えば、同軸ケーブルおよびツイストペアケーブルを含む金属ケーブル類、光通信ケーブル等、または、無線通信媒体、例えば、衛星通信、地上波無線通信等のいずれでもよい。

【0180】

また、搬送波は、データ通信信号を変調するための電磁波または光である。但し、搬送波は直流信号でもよい。この場合にはデータ通信信号は搬送波がないベースバンド波形になる。したがって、搬送波に具現化されたデータ通信信号は、変調されたブロードバンド信号を変調されていないベースバンド信号（電圧0の直流信号を搬送波とした場合に相当）のいずれでもよい。

【0181】

その他、本発明は、上述した実施形態に限定されることなく、本発明の要旨を逸脱しない範囲内で種々の改良・変更が可能である。

（付記1） 自己の通信ネットワークより公開されているサービスに対する不正なアクセスの流入路の探索を行う探索手段と、

前記サービスを前記不正なアクセスから保護するための対策を実施する場所の決定を前記探索の結果に基づいて行う決定手段と、

前記不正なアクセスを自己の通信ネットワークに流入させている流入元で前記対策を実施するとの前記決定に応じて該決定を該流入元へ通知する通知手段と、を有することを特徴とする不正アクセス対処システム。

【0182】

（付記2） 自己の通信ネットワークより公開されているサービスに対する不正なアクセスの流入路の探索を行う探索処理と、

前記サービスを前記不正なアクセスから保護するための対策を実施する場所の決定を前記探索の結果に基づいて行う決定処理と、

前記不正なアクセスを自己の通信ネットワークに流入させている流入元で前記対策を実施するとの前記決定に応じて該決定を該流入元へ通知する通知処理と、をコンピュータに行わせるための不正アクセス対処処理プログラム。

【0183】

（付記3） 前記探索処理は、前記不正なアクセスが検知されたときに前記探索の処理を前記コンピュータに行わせることを特徴とする付記2に記載の不正アクセス対処処理プログラム。

【0184】

（付記4） 前記探索処理は、前記不正なアクセスの検

知が通知されたときに前記探索の処理を前記コンピュータに行わせることを特徴とする付記2に記載の不正アクセス対処処理プログラム。

【0185】

（付記5） 前記探索処理は、前記自己の通信ネットワークで伝送されているトラフィックの監視情報と前記不正なアクセスの内容を示す不正アクセス情報とに基づいて前記流入路を探索する処理を前記コンピュータに行わせることを特徴とする付記2に記載の不正アクセス対処処理プログラム。

【0186】

（付記6） 前記監視情報は、前記自己の通信ネットワークと該自己の通信ネットワークに隣接する通信ネットワークとの境界に配置されている境界ルータの位置情報と、該境界ルータを通過して該自己の通信ネットワークへ流入したトラフィックについての監視情報を少なくとも含むことを特徴とする付記5に記載の不正アクセス対処処理プログラム。

【0187】

20 （付記7） 前記通知処理は、前記不正なアクセスの流入元との間で相互認証を行った後に前記決定を該流入元へ通知する処理を前記コンピュータに行わせることを特徴とする付記2に記載の不正アクセス対処処理プログラム。

【0188】

（付記8） 前記通知処理は、前記不正なアクセスの流入元との間で各々のネットワーク運用におけるセキュリティポリシーに関する情報を交換した後に前記決定を該流入元へ通知する処理を前記コンピュータに行わせることを特徴とする付記2に記載の不正アクセス対処処理プログラム。

【0189】

（付記9） 前記セキュリティポリシーに関する情報は、前記不正なアクセスが検知されなくなってから該不正なアクセスに対する前記対策を解除するまでの時間を示す情報であることを特徴とする付記8に記載の不正アクセス対処処理プログラム。

【0190】

（付記10） 前記セキュリティポリシーに関する情報によって示されている時間が前記自己のネットワークと前記流入元とで異なっているときには、両者のうち短い方の時間を、前記不正なアクセスが検知されなくなってから該不正なアクセスに対する前記対策を解除するまでの時間とすることを特徴とする付記9に記載の不正アクセス対処処理プログラム。

【0191】

（付記11） 前記通知処理は、前記決定と共に、前記不正なアクセスが検知されなくなってから該不正なアクセスに対する前記対策を解除するまでの時間を示す情報を前記流入元へ通知する処理を前記コンピュータに行わ

記対策を実施する決定に応じて該決定を該流入元へ通知する処理を前記コンピュータに行わせる、
ことを特徴とする付記2に記載の不正アクセス対処処理プログラム。

【0203】

(付記23) 前記通知取得処理の実行によって取得された通知が過去に取得されたものと同一の通知であるときに、前記自己の通信ネットワーク若しくは前記他の通信ネットワークより公開されているサービスを該通知に係る不正なアクセスから保護するための対策を該通知の通知元の通信ネットワーク内で実施させる不正アクセス対策実施制御処理を前記コンピュータに更に行わせることを特徴とする付記22に記載の不正アクセス対処処理プログラム。

【0204】

(付記24) 前記通知処理は、前記決定を通知するときに該通知に係る不正なアクセスを一意に特定する情報を併せて通知する処理を前記コンピュータに行わせることを特徴とする付記23に記載の不正アクセス対処処理プログラム。

【0205】

(付記25) 前記通知処理の実行の履歴を記録する記録処理を前記コンピュータに更に行わせることを特徴とする付記2に記載の不正アクセス対処処理プログラム。

【0206】

(付記26) 自己の通信ネットワークより公開されているサービスに対する不正なアクセスの流入路の探索を行い、前記サービスを前記不正なアクセスから保護するための対策を実施する場所の決定を前記探索の結果に基づいて行い、前記不正なアクセスを自己の通信ネットワークに流入させている流入元で前記対策を実施するとの前記決定に応じて該決定を該流入元へ通知することを特徴とする不正アクセス対処方法。

【0207】

(付記27) 自己の通信ネットワークより公開されているサービスに対する不正なアクセスの流入路の探索を行う探索処理と、前記サービスを前記不正なアクセスから保護するための対策を実施する場所の決定を前記探索の結果に基づいて行う決定処理と、前記不正なアクセスを自己の通信ネットワークに流入させている流入元で前記対策を実施するとの前記決定に応じて該決定を該流入元へ通知する通知処理と、をコンピュータに行わせるための不正アクセス対処処理プログラムを記録した該コンピュータで読み取り可能な記録媒体。

【0208】

【発明の効果】

以上詳細に説明したように、本発明は、自己の通信ネットワークより公開されているサービスに対する不正なアクセスの流入路を探査し、このサービスをこの不正なアクセスから保護するための対策を実施する場所の決定をこの探査の結果に基づいて行い、この不正なアクセスを自己の通信ネットワークに流入させている流入元でこの対策を実施するとの決定に応じて該決定を該流入元へ通知する。

【0209】

10 こうすることにより、本発明によれば、不正アクセスの発信元にできるだけ近い場所での不正アクセス対策の実施が可能となる結果、分散型サービス不能化攻撃に効果的に対処することができるという効果を奏す。

【図面の簡単な説明】

【図1】本発明の原理構成を示す図である。

【図2】本発明を実施する不正アクセス対処システムの機能構成を示す図である。

【図3】図2のシステムで使用されるコンピュータのハードウェア構成例を示す図である。

20 【図4】トラフィックモニター手順の内容を示す図である。

【図5】トラフィックDBのデータ構造を示す図である。

【図6】不正アクセス通知手順の内容を示す図である。

【図7】不正アクセス通知のデータ形式を示す図である。

【図8】不正アクセス対策制御手順の内容を示す図である。

30 【図9】不正アクセス対策実施場所決定手順の内容を示す図である。

【図10】不正アクセス対策実施手順の内容を示す図である。

【図11】組織間認証手順の内容を示す図である。

【図12】組織間ポリシー交換手順の内容を示す図である。

【図13】不正アクセス対策記録手順の内容を示す図である。

【図14】記録させた制御プログラムをコンピュータで読み取ることの可能な記録媒体の例を示す図である。

40 【図15】従来の不正アクセス対処システムの概略を説明する図である。

【符号の説明】

10 自ISP

11、501 運用管理システム

12、100 不正アクセス対策マネージャサイト

12-1 探索手段

12-2 決定手段

12-3 通知手段

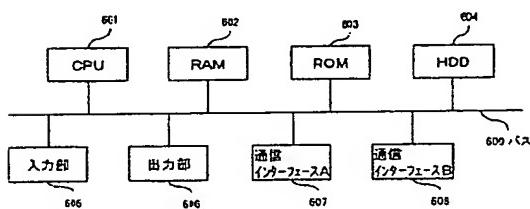
12-4 認証手段

50 12-5 セキュリティポリシー交換手段

37

- 12-6 不正アクセス対策実施制御手段
 12-7 通知取得手段
 12-8 記録手段
 13、200 不正アクセス通知エージェントサイト
 13-1 不正アクセス通知手段
 14、502 IDS
 15 顧客境界ルータ
 16、18、300 不正アクセス対策実施エージェントサイト
 16-1、18-1 トラフィックモニター手段
 16-2、18-2 不正アクセス対策実施手段
 17、2002、2003 ISP境界ルータ
 19、3001、4001 POP境界ルータ
 20、1000 顧客サイト
 21、1001 Webシステム
 22、1002 ファイヤウォール
 30 隣接ISP
 40 非常時接続利用者端末
 101 管理端末
 110 不正アクセス対策マネージャプログラム
 111 不正アクセス対策制御部
 112 不正アクセス対策記録制御部
 113、313 IO制御部
 120 証明書
 130 Policy
 140 Log DB
 210 不正アクセス通知プログラム

【図3】

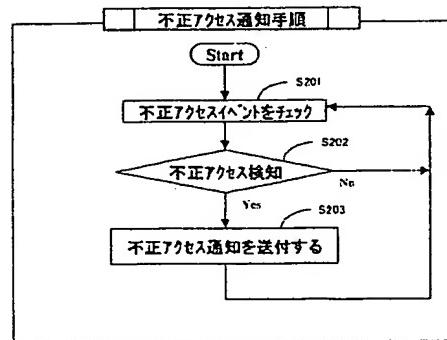
図2のシステムで使用されるコンピュータの
ハードウェア構成例を示す図

38

- 211 不正アクセス通知エンジン
 212 通信制御部
 310 不正アクセス対策実施プログラム
 311 不正アクセス対策実施エンジン
 312 トラフィックモニターエンジン
 320 トラフィックDB
 400 不正アクセス対処システム専用ネットワーク
 500 ISPネットワーク
 503、2001 境界ルータ
 10 601 CPU
 602 RAM
 603 ROM
 604 HDD
 605 入力部
 606 出力部
 607 通信インターフェースA
 608 通信インターフェースB
 609 バス
 701 コンピュータ
 20 702 メモリ
 703 可搬型記録媒体
 704 回線
 705 プログラムサーバ
 706 記憶装置
 2000 ISP-A
 3000 ISP-B
 4000 ISP-C

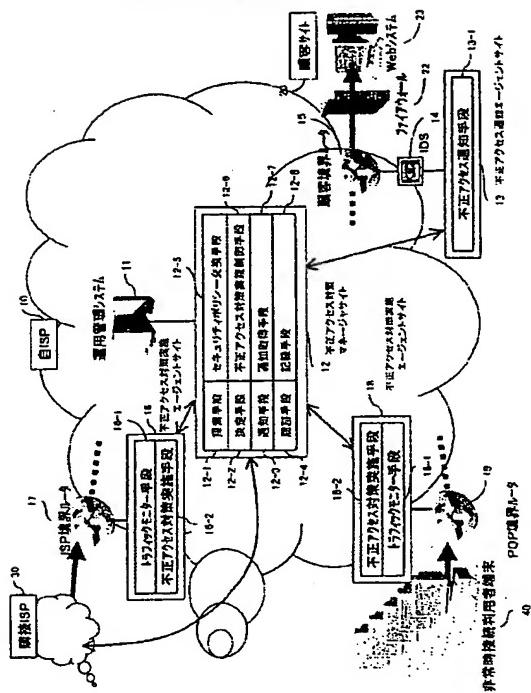
【図6】

不正アクセス通知手順の内容を示す図



【図1】

本発明の原理構成を示す図



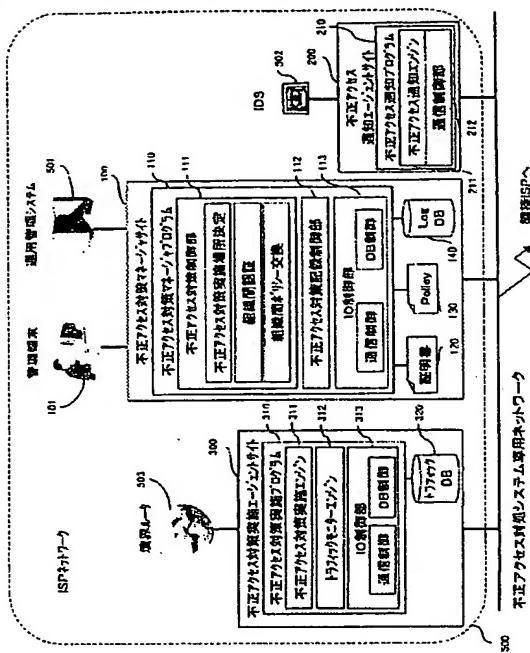
【図7】

不正アクセス通知のデータ形式を示す図

データメンバー	例1	例2
検知 ID	00-00-0E-82-2E-74-001	00-00-0E-82-2E-74-002
時刻レンジスタート (GMT)	2003/2/1 16:01:16	2003/2/17 11:31:11
時刻レンジエンド (GMT)	2003/2/1 16:11:16	2003/2/17 11:41:11
攻撃種別	TCP Syn Flood	Worm
組織名	Company A	Company B
所属 ISP	ISP ABC	ISP XYZ
ターゲットプロトコル	TCP	UDP
Src IP	10.4.120.2	169.0.255.0
Dist IP	192.168.X.Y	164.71.A.B
Dist Port	80	1434
不正パケット数	156789	876534
攻撃ツール名	TFN2K	SOL Slammer
対策解除ポリシー	10分	20分

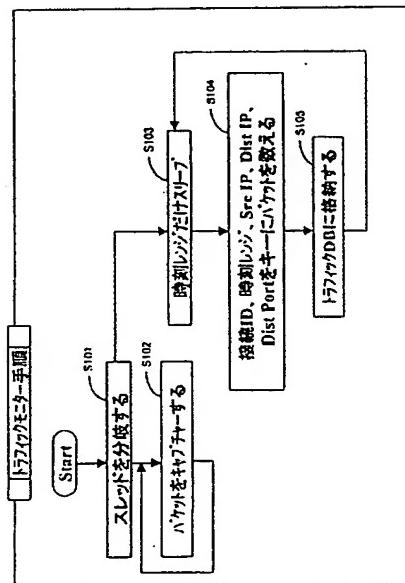
【図2】

本発明を実施する不正アクセス対処システムの機能構成を示す図



【図4】

トラフィックモニター手順の内容を示す図



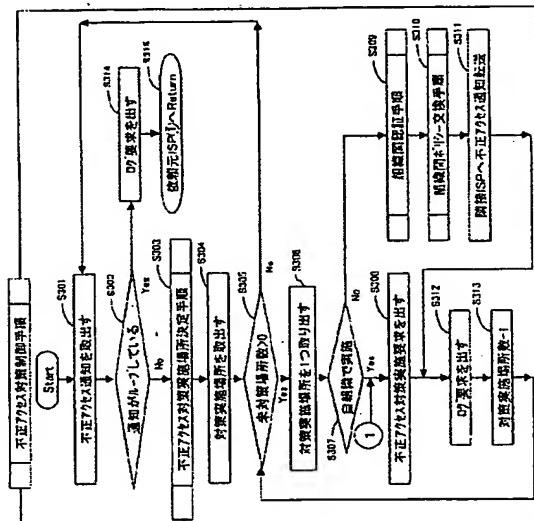
[图 5]

トライックDBのデータ構造を示す図

接続ID	接続名	Src IP	Dst IP	Dst Port	Count
ADC01234	IP:10.10.10.10	202.248.20.234	202.248.20.68	80	1458
NBC567890	IP:10.10.10.10	202.248.20.112	202.248.20.68	80	16724
AS2456	IP:10.10.10.10	10.34.105.194	202.248.20.68	80	168143

【図8】

不正アクセス対策制御手順の内容を示す図

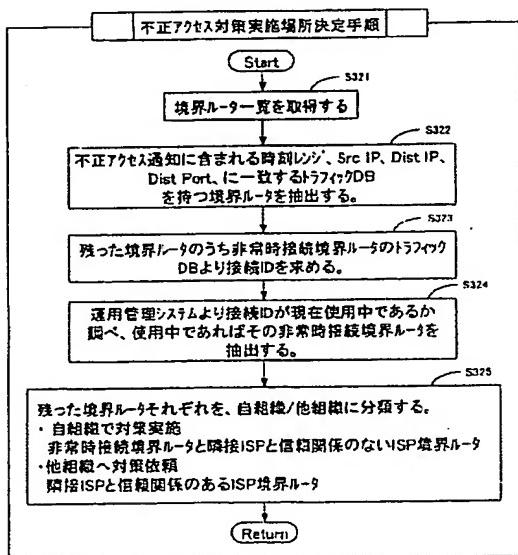


〔四〕 10

不正アクセス対策実施手順の内容を示す図

(图 9)

不正アクセス対策実施場所決定手順の内容を示す図



```

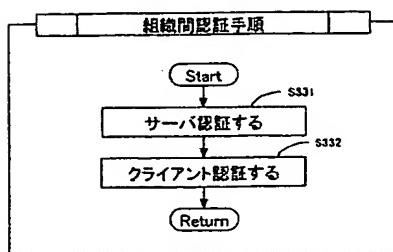
graph TD
    Start([Start]) -- S401 --> Req[不正アクセス対策実施要否を割り出す]
    Req -- S402 --> Admin[通常管理: ハルにより接続規制固有の情報を入手する]
    Admin -- S403 --> IP[不正アクセスに含まれる元IP、Diat IP、Dist Port、接続別情報等を元に、ハルを認定する]
    IP -- S404 --> Check[判定結果監視用レコードを分岐する]
    Check -- No --> S405[ハルの状況を貯め出す]
    S405 -- S406 --> Decision{接続終了時間閾値を越えず不正アクセスであるかがハルが来ていないか}
    Decision -- No --> S407[ハルを解禁する]
    S407 -- S408 --> ReqOut[0]の要求を出す
    ReqOut -- S409 --> Exit([Exit])
    Decision -- Yes --> S408

```

The flowchart details the process for handling unauthorized access to system resources. It starts with an initial state, followed by determining if action is required for unauthorized access. If required, it involves administrative management (getting specific information from Haru), identifying the unauthorized access (by IP, Diat IP, Dist Port, and connection-specific information), and then branching to check the monitoring results. If the result is 'No' (the user has not exceeded the connection end time limit and has not left), the user's status is stored (S405). If the result is 'Yes' (the user has exceeded the limit or left), the user is released (S407). Finally, a request is issued (S408), which leads to the exit state (S409).

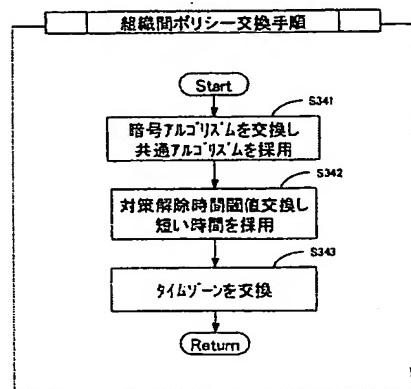
【図11】

組織間認証手順の内容を示す図



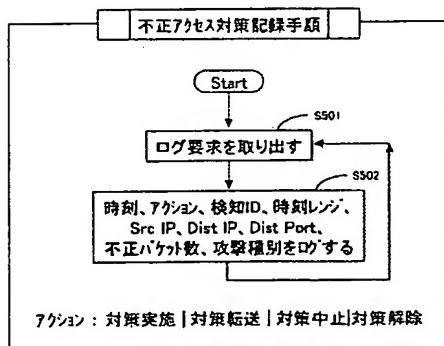
【図12】

組織間ポリシー交換手順の内容を示す図

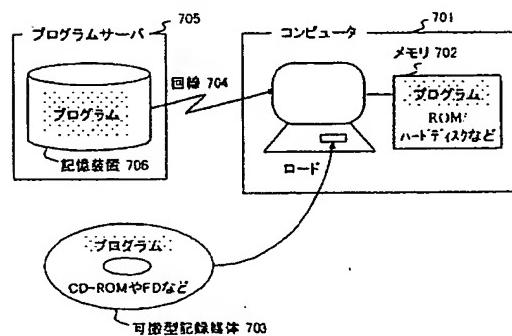


【図13】

不正アクセス対策記録手順の内容を示す図

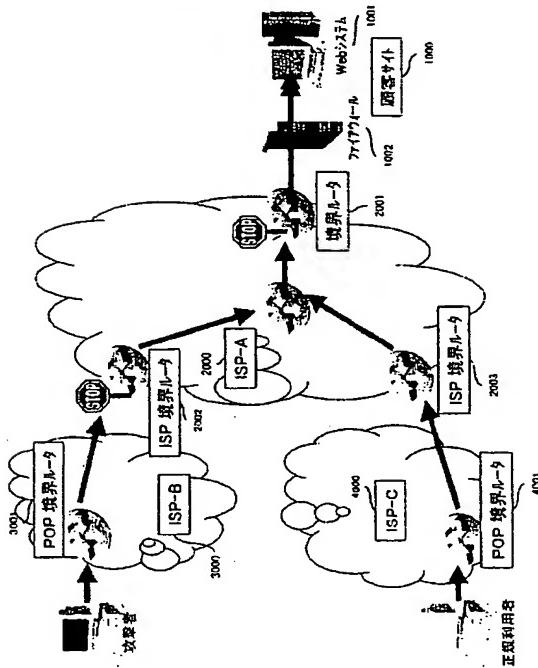


【図14】

記録させた制御プログラムをコンピュータで
読み取ることの可能な記録媒体の例を示す図

【図15】

従来の不正アクセス対処システムの概略を説明する図



フロントページの続き

(72)発明者 森田 真由子

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

(72)発明者 鳥居 悟

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

(72)発明者 小谷野 修

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

Fターム(参考) 5B085 AA08 AC16 BG02 CA02 CA04

5B089 GB02 KA17 MC02 MC06 MC08

5K030 GA15 HA08 JA10 LC13

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.